

Systemové programování Windows

Data Protection API

DPAPI

- ▶ Ochrana dat bez nutnosti použití kryptografických funkcí
- ▶ První verze se nepovedly - W2k



DPAPI - zašifrování

```
▶ BOOL WINAPI CryptProtectData (
    _In_      DATA_BLOB *pDataIn,
    _In_      LPCWSTR  szDataDescr,
    _In_      DATA_BLOB *pOptionalEntropy,
    _In_      PVOID    pvReserved,
    _In_opt_  CRYPTPROTECT_PROMPTSTRUCT *pPromptStruct,
    _In_      DWORD    dwFlags,
    _Out_     DATA_BLOB *pDataOut );
```

```
typedef struct _CRYPTOAPI_BLOB {
    DWORD cbData;
    BYTE  *pbData;
} DATA_BLOB;
```



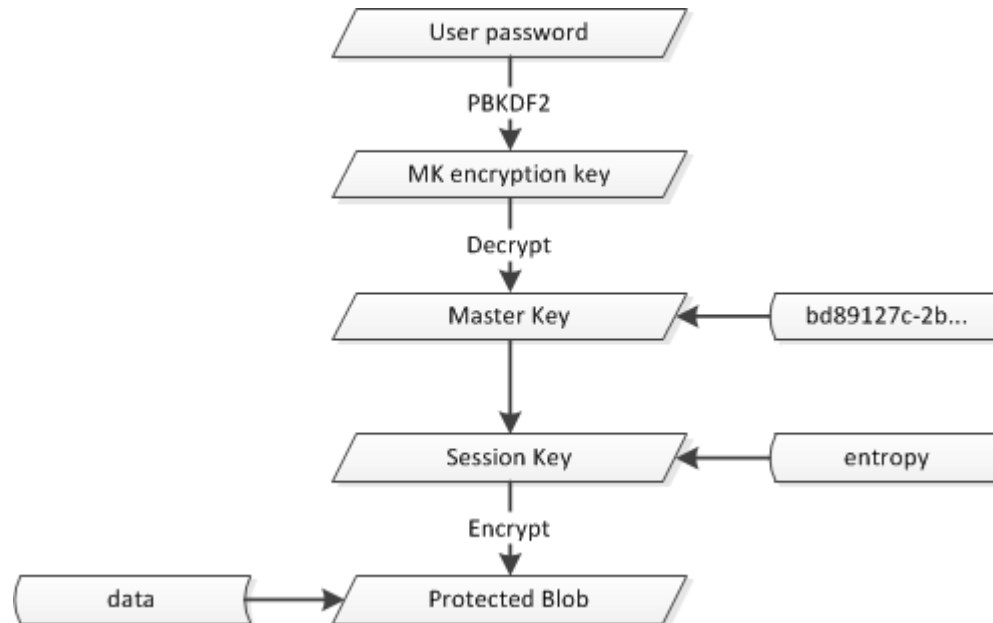
DPAPI - dešifrování

```
BOOL WINAPI CryptUnprotectData(  
    _In_          DATA_BLOB *pDataIn,  
    _Out_opt_    LPWSTR *ppszDataDescr,  
    _In_opt_     DATA_BLOB *pOptionalEntropy,  
    _Reserved_   PVOID pvReserved,  
    _In_opt_     CRYPTPROTECT_PROMPTSTRUCT *pPromptStruct,  
    _In_         DWORD dwFlags,  
    _Out_        DATA_BLOB *pDataOut );
```



DPAPI

- ▶ Provádí se v Local System Authority (LSA) procesu
- ▶ Data-flow



Master Key

- ▶ Umístění
 - ▶ ...\Users\..\AppData\Roaming\Microsoft\Protect\SID\...
- ▶ Master Key se mění každých 90 dní



Parametry

▶ Password guess speed

OS	Encryption algorithm	Hash algorithm	Number of iterations in PKCS#5 PBKDF2	Password guess speed (pwd/sec)
Windows2000	RC4	SHA1	1	95000
WindowsXP	3DES	SHA1	4000	76
WindowsVista	3DES	SHA1	24000	12
Windows7	AES256	SHA512	5600	10

Zdroj: <http://www.passcape.com/index.php?section=docsys&cmd=details&id=28>

▶ Změna hesla nemá žádný dopad

- ▶ Řetězec CREDHIST záznamů
- ▶ Stačí znát poslední heslo

▶ Obsahuje

- ▶ User Master Key
- ▶ Domain Backup Key
- ▶ ...



Je dobré si uvědomit

- ▶ Kdo zná heslo je schopen dešifrovat Protected Data Blob (PDB)
 - ▶ „Šikovný“ admin
 - ▶ Password Reset Disk
- ▶ Nedoménové PC
 - ▶ Force restart hesla znemožní dešifrovat PDB
- ▶ Doménové PC
 - ▶ Domain Master Key lze dešifrovat „domluvou“ s Active Directory.
 - ▶ Force restart hesla nemá žádný dopad.
- ▶ dwFlags CRYPTPROTECT_LOCAL_MACHINE vynutí použití Local Master Key



Díky za pozornost

